FortiOS v4.0 MR3 Patch Release 10

Release Notes

FortiOS v4.0 MR3 Patch Release 10 Release Notes

September 10, 2012

01-4310-180542-20120910

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log

Date	Change Description
2012-09-10	Initial release.
2012-09-13	Removed reference to FortiGate 1240B CSB and Special Notice.
2012-09-17	Updated Resolved Issues section.
2012-10-04	FortiGate 300C compatibility section added to Special Notices.

Introduction

This document provides installation instructions and addresses issues and caveats in FortiOS v4.0 MR3 Patch Release 10 build 0639.

Table 1 outlines the release status for these models.

Table 1: Supported models

FortiGate Models	**FortiOS v4.0 MR3 Patch Release 10**
FG-20C, FG-30B, FG-40C, FG-50B, FG-51B, FG-60B, FG-60C, FG-80C, FG-80CM, FG-82C, FG-100A, FG-100D, FG-110C, FG-111C, FG-200A, FG-200B, FG-200B-PoE, FG-224B, FG-300A, FG-300C, FG-310B, FG-310B-DC, FG-311B, FG-400A, FG-500A, FG-600C, FG-620B, FG-620B-DC, FG-621B, FG-800, FG-800C, FG-800F, FG-1000A, FG-1000A-FA2, FG-1000A-LENC, FG-1000C, FG-1240B, FG-3016B, FG-3040B, FG-3140B, FG-3600, FG-3600A, FG-3810A, FG-3950B, FG-3951B, FG-5001, FG-5001A, FG-5001B, FG-5001FA2, FG-5002FB2, FG-5005FA2, FG-5101C, and FG-One.	All models are supported on the regular v4.0 MR3 Patch Release 10 branch.
FortiWiFi Models	**FortiOS v4.0 MR3 Patch Release 10**
FWF-20C, FWF-30B, FWF-40C, FWF-50B, FWF-60B, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-80CM, FWF-81CM	All models are supported on the regular v4.0 MR3 Patch Release 10 branch.
FortiGate Virtual Machine Models	**FortiOS v4.0 MR3 Patch Release 10**
FortiGate VM32, VM-64 and VM64-XEN	All models are supported on the regular v4.0 MR3 Patch Release 10 branch.
FortiSwitch Model	**FortiOS v4.0 MR3 Patch Release 10**
FortiSwitch 5203B Networking/Security Blade	This model is supported on the regular v4.0 MR3 Patch Release 10 branch.

Table 2 lists the supported virtualization software for this release.

Table 2: Supported virtualization software

Virtualization Software	**FortiOS v4.0 MR3 Patch Release 10**
vSphere 4.0, 4.1, vSphere 5.0 Citrix XenServer 5.6sp2/6.0 Open Source Xen 3.4.3 Open Source Xen 4.1	All models are supported by the regular v4.0 MR3 Patch Release 10 branch. See “Limitations” on page 20 for more information.

See http://docs.fortinet.com/fgt.html for additional documents on FortiOS v4.0 MR3.

FortiOS Carrier

This chapter provides platform support information for FortiOS Carrier v4.0 MR3 Patch Release 10 build 0639.

Table 3 outlines the release status for these models.

Table 3: Supported models

FortiCarrier Models	FortiOS Carrier v4.0 MR3 Patch Release 10
FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001, FCR-5001A, FCR-5001B, FCR-5001FA2, and FCR-5005FA2. Firmware image filenames begin with FK.	All models are supported on the regular v4.0 MR3 Patch Release 10 branch.

See http://docs.fortinet.com/fgt.html for additional documents on FortiCarrier v4.0 MR3.

Special Notices

General

The TFTP boot process erases all current firewall configuration and replaces it with the factory default settings.

Important

Monitor settings for Web-based Manager access

Fortinet recommends setting your monitor to a screen resolution of 1280x1024. This allows for all the objects in the Web-based Manager to be viewed properly.

Supported web browsers

- Microsoft Internet Explorer 8.0 and 9.0
- Mozilla FireFox 13.0 and 14.0

Before any upgrade

Save a copy of your FortiGate unit configuration (including replacement messages) prior to upgrading.

After any upgrade

If you are using the Web-based Manager, clear the browser cache prior to login on the FortiGate to ensure the Web-based Manager screens are displayed properly.

The Virus and Attack definitions included with an image upgrade may be older than ones currently available from the Fortinet's FortiGuard Distribution Server. Fortinet recommends performing an Update Now (*System* > *Config* > *FortiGuard* > *AntiVirus and IPS Options*) as soon as possible after upgrading. Consult the FortiOS Handbook/FortiOS Carrier Handbook for detailed procedures.

FortiGate 100D hardware compatibility

FortiOS v4.0 MR3 Patch Release 10 contains a compatibility issue with certain units of the FortiGate 100D. Units that are affected have a system part number of P11510-02 and later. You can view the system part number on the bottom of the unit or with the `get system status` CLI command. Units with this system part number must run FortiOS v4.0 MR3 Patch Release 7.

This will be addressed in FortiOS v4.0 MR3 Patch Release 11.

FortiGate 300C hardware compatibility

FortiOS v4.0 MR3 Patch Release 10 contains a compatibility issue with certain units of the FortiGate 300C. Units that are affected have a system part number of P09616-05 and later. You can view the system part number on the bottom of the unit or from the `get system status` CLI command. Units with this system part number must run FortiOS v4.0 MR3 Patch Release 8.

This will be addressed in FortiOS v4.0 MR3 Patch Release 11.

FortiGate 1240B upgrade and downgrade limitations

With the release of FortiOS v4.0 MR3 Patch Release 2 and later, the FortiGate 1240B will run a 64-bit version of FortiOS. This has introduced certain limitations on upgrading firmware in a high availability (HA) environment, and downgrading.

When performing an upgrade from a 32-bit FortiOS version to a 64-bit FortiOS version, and the FortiGate 1240Bs are running in a HA environment with the uninterruptable-upgrade option enabled, the upgrade process may fail on the primary device after the subordinate devices have been successfully upgraded. To work around this situation, users may disable the uninterruptable-upgrade option to allow all HA members to be successfully upgraded. Without the uninterruptable-upgrade feature enabled, several minutes of service unavailability are to be expected.

Downgrading a FortiGate 1240B from FortiOS v4.0 MR3 Patch Release 2 is not supported due to technical limitations between 64-bit and 32-bit versions of FortiOS. The only procedure to downgrade firmware is by using the TFTP server and BIOS menu to perform the downgrade. In this case the configuration will need to be restored from a previously backed up version.

Upgrade Information

Upgrading from FortiOS v4.0 MR3

FortiOS v4.0 MR3 Patch Release 10 build 0639 officially supports upgrade from FortiOS v4.0 MR3 GA or later.

Historical reports upgrade limitation

For the following units, historical reports from previous builds will not be retained after upgrading to FortiOS v4.0 MR3 Patch Release 10:

- FortiGate 20C
- FortiWiFi 20C
- FortiGate 40C
- FortiWiFi 40C
- FortiGate 60C
- FortiWiFi 60C
- FortiWiFi 60CM
- FortiWiFi 60CX-ADSL-A
- FortiGate 80C
- FortiWiFi 81CM

Workaround: Download the historical reports to a local PC hard drive before performing the upgrade.

SQL logging upgrade limitation

For the following units, after upgrading to FortiOS v4.0 MR3 Patch Release 10, SQL logging will be retained based on the total size of the RAM available on the device. Logs will use up to maximum of 10% of the RAM, once passed that threshold, any new logs will start to overwrite the older logs. The historical report generation will also be affected based on the SQL logs that are available for query.

- FortiGate 100D
- FortiGate 300C

FortiGate 100D

FortiOS v4.0 MR3 Patch Release 10 supports the FortiGate 100D platform. Included with this model is a special purpose management port that operates on its own virtual domain (VDOM).

An issue exists with this feature whereby FortiCare registration fails when initiated from the FortiGate device if this port is connected to the Internet and thus FortiGuard and FortiCare.

Upgrading the FortiOS image from its factory default image (build 4083) to FortiOS v4.0 MR2 Patch Release 12 or later does not switch the management VDOM. You must change the management VDOM from the default setting to the root VDOM.

To do this, use the following CLI commands:

```
config system global
  set management-vdom root
end
end
```

Upgrading from FortiOS v4.0 MR2

Please upgrade to the latest v4.0 MR2 patch release prior to upgrading to v4.0 MR3 Patch Release 10. For more information, see the latest FortiOS v4.0 MR2 patch release notes.

After every upgrade, ensure that the build number and branch point match the image that was loaded.

DDNS

DDNS configurations under `interface` are moved to global mode `config system ddns` after upgrading to FortiOS v4.0 MR2 Patch Release 12.

DNS server

`dns-query recursive/non-recursive` option under specific interfaces are moved to the system level per VDOM mode, and `config system dns-server` can be used to configure the option after upgrading to FortiOS v4.0 MR2 Patch Release 12.

Ping server

`gwdetect` related configurations under specific interfaces are moved under router per VDOM mode, and `config router gwdetect` can be used to configure the option after upgrading to FortiOS v4.0 MR2 Patch Release 12.

Central-management

`set auto-backup disable` and `set authorized-manager-only enable` configurations under `config system central-management` are removed after upgrading to FortiOS v4.0 MR2 Patch Release 12.

SNMP community

A 32 bits network mask will be added to an IP address of SNMP host upon upgrading to FortiOS v4.0 MR2 Patch Release 12.

Modem settings

`wireless-custom-vendor-id` and `wireless-custom-product-id` are moved from `config system modem` to `config system 3g-modem custom` after upgrading to FortiOS v4.0 MR2 Patch Release 12.

AMC slot settings

The default value of `ips-weight` under `config system amc-slot` will be changed from `balanced` to `less-fw` after upgrading to FortiOS v4.0 MR2 Patch Release 12.

Wireless radio settings

Wireless radio settings, except for SSID, Security Mode, and Authentication settings, will be lost after upgrading.

Web filter overrides

The contents of Web Filter overrides will be lost after upgrading from FortiOS v4.0 MR2 Patch Release 4 build 0313 to FortiOS v4.0 MR2 Patch Release 12.

Firewall policy settings

If the source interface or destination interface is set as the `amc-XXX` interface, the default value of `ips-sensor` under `config firewall policy` is changed from `all_default` to `default` after upgrading to FortiOS v4.0 MR2 Patch Release 12.

URL filter

The `action` options in the urlfilter configuration have been changed from `Allow`, `Pass`, `Exempt`, and `Block` to `Allow`, `Monitor`, `Exempt`, and `Block`. The `Allow` action will not report log in FortiOS v4 MR3 Patch Release 1. The `Monitor` action will act as the function that allows log reporting. The `Pass` action in FortiOS v4.0 MR2 has been merged with `Exempt` in FortiOS v4.0 MR3 Patch Release 1, and the CLI command has been changed from `set action pass` to `set exempt pass`.

FortiGuard log filter

The settings of `config log fortiguard filter` are removed after upgrading to FortiOS v4.0 MR2 Patch Release 12.

FortiGuard log setting

The options `quotafull` and `use-hdd` in `config log fortiguard setting` are removed upon upgrading to FortiOS v4.0 MR2 Patch Release 12.

Upgrading from FortiOS v4.0 MR1

Upgrading from FortiOS v4.0 MR1 is not supported. Please upgrade to FortiOS v4.0 MR3 Patch Release 5 prior to upgrading to v4.0 MR3 Patch Release 10. For more information, see the FortiOS v4.0 MR3 Patch Release 5 Release Notes.

Downgrading to FortiOS v4.0 MR1

Downgrading to FortiOS v4.0 MR1 (or later) results in configuration loss on ALL models. Only the following settings are retained:

- operation modes
- interface IP/management IP
- route static table
- DNS settings
- VDOM parameters/settings
- admin user account
- session helpers
- system access profiles.

Product Integration

FortiManager support

FortiOS v4.0 MR3 Patch Release 10 is supported by FortiManager v4.0 MR3 Patch Releases 6 and later.

FortiAnalyzer support

FortiOS v4.0 MR3 Patch Release 10 is supported by FortiAnalyzer v4.0 MR3.

If you are using a FortiAnalyzer unit running FortiAnalyzer v4.0 MR2, you must upgrade it to FortiAnalyzer v4.0 MR3. FortiAnalyzer units running FortiAnalyzer v4.0 MR2 will not function correctly with FortiOS v4.0 MR3 Patch Release 10.

FortiClient support

FortiOS v4.0 MR3 Patch Release 10 is fully compatible with FortiClient v4.0 MR2 Patch Release 3 and later.

FortiOS v4.0 MR3 Patch Release 10 is supported by FortiClient v4.0 MR3 for the following:

- Microsoft Windows XP 32-bit
- Microsoft Windows Vista 32-bit
- Microsoft Windows Vista 64-bit
- Microsoft Windows 7 32-bit
- Microsoft Windows 7 64-bit

FortiAP support

FortiOS v4.0 MR3 Patch Release 10 supports the following FortiAP models:

- FortiAP 210B
- FortiAP 220A
- FortiAP 220B
- FortiAP 221B
- FortiAP 222B

The FortiAP devices must be running FortiAP v4.0 MR3 and later.

Fortinet Single Sign-On (FSSO) support

FortiOS v4.0 MR3 Patch Release 10 is supported by FSSO v4.0 MR3 build 0124 for the following:

- Microsoft Windows Server 2003 R2 32-bit
- Microsoft Windows Server 2003 R2 64-bit
- Microsoft Windows Server 2008 32-bit
- Microsoft Windows Server 2008 64-bit
- Microsoft Windows Server 2008 R2 64-bit
- Novell eDirectory 8.8.

IPv6 currently is not supported by FSSO.

FortiExplorer support

FortiOS v4.0 MR3 Patch Release 10 is supported by FortiExplorer v1.8 build 1427.

AV Engine and IPS Engine support

FortiOS v4.0 MR3 Patch Release 10 is supported by AV Engine v4.0 MR3 build 0398 and IPS Engine v1.0 build 0247.

Module support

FortiOS v4.0 MR3 Patch Release 10 supports Advanced Mezzanine Card (AMC), Fortinet Mezzanine Card (FMC), Rear Transition Modules (RTM), and Fortinet Storage Module (FSM) removable modules. These modules are not hot swappable. The FortiGate unit must be turned off before the module is inserted or removed.

Table 4 outlines supported modules.

Table 4: Supported modules

AMC/FMC/FSM/RTM Modules	FortiGate Models
Storage Module 500GB HDD Single-Width AMC (ASM-S08)	FG-310B, FG-620B, FG-621B, FG-3016B, FG-3600A, FG-3810A, FG-5001A-SW
Storage Module 64GB SSD Fortinet Storage Module (FSM-064)	FG-200B, FG-311B, FG-1240B, FG-3040B, FG-3140B, FG-3951B
Accelerated Interface Module 4xSFP Single-Width AMC (ASM-FB4)	FG-310B, FG-311B, FG-620B, FG-621B, FG-1240B, FG-3016B, FG-3600A, FG-3810A, FG-5001A-SW
Accelerated Interface Module 2x10-GbE XFP Double-Width AMC (ADM-XB2)	FG-3810A, FG-5001A-DW
Accelerated Interface Module 8xSFP Double-Width AMC (ADM-FB8)	FG-3810A, FG-5001A-DW
Bypass Module 2x1000 Base-SX Single-Width AMC (ASM-FX2)	FG-310B, FG-311B, FG-620B, FG-621B, FG-1240B, FG-3016B, FG-3600A, FG-3810A, FG-5001A-SW

Table 4: Supported modules (continued)

Bypass Module 4x10/100/1000 Base-T Single-Width AMC (ASM-CX4)	FG-310B, FG-311B, FG-620B, FG-621B, FG-1240B, FG-3016B, FG-3600A, FG-3810A, FG-5001A-SW
Security Processing Module 2x10/100/1000 SP2 Single-Width AMC (ASM-CE4)	FG-1240B, FG-3810A, FG-3016B, FG-5001A-SW
Security Processing Module 2x10-GbE XFP SP2 Double-Width AMC (ADM-XE2)	FG-3810A, FG-5001A-DW
Security Processing Module 4x10-GbE SFP+ Double-Width AMC (ADM-XD4)	FG-3810A, FG-5001A-DW
Security Processing Module 8xSFP SP2 Double-Width AMC (ADM-FE8)	FG-3810A
Rear Transition Module 10-GbE backplane fabric (RTM-XD2)	FG-5001A-DW
Security Processing Module (ASM-ET4)	FG-310B, FG-311B
Rear Transition Module 10-GbE backplane fabric (RTM-XB2)	FG-5001A-DW
Security Processing Module 2x10-GbE SFP+ (FMC-XG2)	FG-3950B, FG-3951B
Accelerated Interface Module 2x10-GbE SFP+ (FMC-XD2)	FG-3950B, FG-3951B
Accelerated Interface Module 20xSFP (FMC-F20)	FG-3950B, FG-3951B
Accelerated Interface Module 20x10/100/1000 (FMC-C20)	FG-3950B, FG-3951B
Security Processing Module (FMC-XH0)	FG-3950B

SSL-VPN support

SSL-VPN standalone client

FortiOS v4.0 MR3 Patch Release 10 supports the SSL-VPN tunnel client standalone installer build 2270 for the following:

- Windows in .exe and .msi format
- Linux in .tar.gz format
- Virtual Desktop in .jar format for Windows 7
- Mac OS X 10.7 in .dmg format

Table 5 lists the supported operating systems.

Table 5: Supported operating systems

Windows	Linux	Mac OS X
Windows XP 32-bit SP3	CentOS 5.6	Lion 10.7
Windows 7 32-bit SP1		
Windows 7 64-bit SP1		
Virtual Desktop Support		
Windows 7 32-bit SP1		

SSL-VPN web mode

FortiOS v4.0 MR3 Patch Release 10 supports the following browsers for SSL-VPN web mode:

- Internet Explorer 8.0
- Internet Explorer 9.0
- Firefox 13.0
- Firefox 3.6
- Safari 5.1

SSL-VPN host compatibility list

The following tables list the AntiVirus and Firewall client software packages that are supported.

Table 6 lists supported Windows XP AntiVirus and Firewall software.

Table 6: Supported Windows XP AntiVirus and Firewall software

Product	AntiVirus	Firewall
Symantec Endpoint Protection v11	✔	✔
Kaspersky AntiVirus 2009	✔	
McAfee Security Center v8.1	✔	✔
Trend Micro Internet Security Pro	✔	✔
F-Secure Internet Security 2009	✔	✔

Table 7 lists supported Windows 7 32-bit AntiVirus and Firewall software.

Table 7: Supported Windows 7 32-bit AntiVirus and Firewall software

Product	AntiVirus	Firewall
CA Internet Security Suite Plus Software	✔	✔
AVG Internet Security 2011		
F-Secure Internet Security 2011	✔	✔
Kaspersky Internet Security 2011	✔	✔
McAfee Internet Security 2011	✔	✔
Norton 360™ Version 4.0	✔	✔
Norton™ Internet Security 2011	✔	✔
Panda Internet Security 2011	✔	✔
Sophos Security Suite	✔	✔
Trend Micro Titanium Internet Security	✔	✔
ZoneAlarm Security Suite	✔	✔
Symantec Endpoint Protection Small Business Edition 12.0	✔	✔

Table 8 lists supported Windows 7 64-bit AntiVirus and Firewall software.

Table 8: Supported Windows 7 64-bit AntiVirus and Firewall software

Product	AntiVirus	Firewall
CA Internet Security Suite Plus Software	✔	✔
AVG Internet Security 2011		
F-Secure Internet Security 2011	✔	✔
Kaspersky Internet Security 2011	✔	✔
McAfee Internet Security 2011	✔	✔
Norton 360™ Version 4.0	✔	✔
Norton™ Internet Security 2011	✔	✔
Panda Internet Security 2011	✔	✔
Sophos Security Suite	✔	✔
Trend Micro Titanium Internet Security	✔	✔
ZoneAlarm Security Suite	✔	✔
Symantec Endpoint Protection Small Business Edition 12.0	✔	✔

Explicit Web Proxy browser support

The following browsers are supported by the Explicit Web Proxy feature:

- Microsoft Internet Explorer 7.0
- Microsoft Internet Explorer 8.0
- Mozilla Firefox 3.x

Resolved Issues

The resolved issues listed below do not list every bug that has been corrected with this release. For inquires about a particular bug, please contact Customer Support.

The following sections list the resolved issues for FortiOS v4.0 MR3 Patch Release 10:

SSL-VPN

Table 9: Resolved SSL-VPN issues

Bug ID	Description
179112	Buffer overflow in SSL VPN URL check. A buffer overflow may occur when a specific SSL VPN URL parameter is crafted to an invalid length. Exploitation to grant system access may be possible, however would require an attacker to have valid VPN credentials or carry out a specific brute force attack.
179936	Buffer overflow in SSL VPN parameter. A buffer overflow may occur when manipulating a parameter in the header of a SSL VPN connection. For proper exploitation to occur, an attacker would have to be logged into the SSL VPN.

System

Table 10: Resolved System issues

Bug ID	Description
177343	Disable factory license feature on models using NAND flash.

Limitations

This section outlines the limitations in FortiOS v4.0 MR3 Patch Release 10.

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

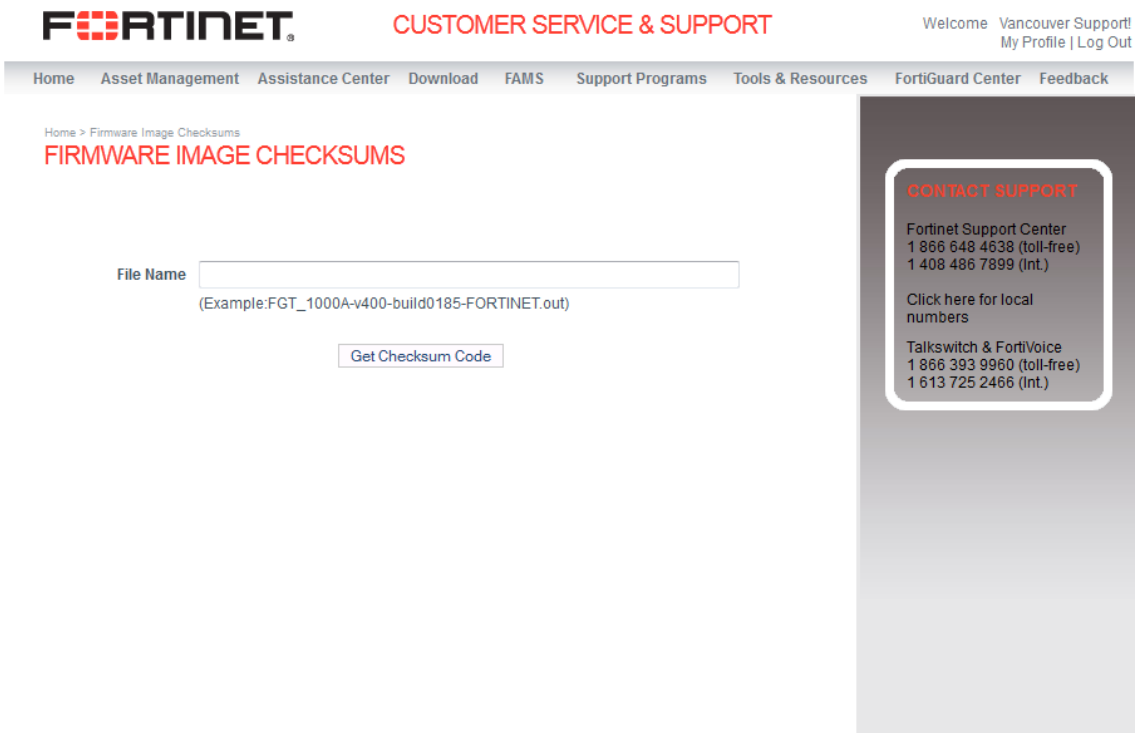
Open Source Xen limitations

When using Ubuntu 11.10, Xen 4.1.0, and libvir 0.9.2, importing issues may arise when using the qcow2 format and existing HDA issues.

Image Checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support website located at https://support.fortinet.com. After logging in, click on *Download* > *Firmware Image Checksum*, enter the image file, including the extension, and select *Get Checksum Code*.

Figure 1: Customer Service & Support image checksum tool



End of Release Notes